

NEED TO KNOW

a national security newsletter

Volume 5, Number 2

May 2005

Low-Enriched Fuel Development

Meeting great issues head on

More than 100 years ago, Theodore Roosevelt said, "If we are to be really great people, we must strive in good faith to play a great part in the world. We cannot avoid meeting great issues. All that we can determine for ourselves is whether we shall meet them well or ill."

The United States and the international community face a great issue today – the threat of nuclear and radiological materials falling into terrorist hands.

Former Secretary of Energy Spencer Abraham tackled the issue head on when he launched the Global Threat Reduction Initiative in May 2004.



In a speech to the International Atomic Energy Agency, Abraham said, "Saying you want to make the world a safer place is simple.

The challenge of actually doing that is the hard part."

See **FUEL**, page 2

Pat Hallinan operates a friction stir welder, which bonds aluminum to the fuel during the fuel fabrication process.



State of the Division

Dr. KP Ananth,
*Associate Laboratory Director,
National and Homeland Security*

It's not often a new national laboratory is launched, which makes the recent startup of Idaho National Laboratory a highly significant milestone. In Laboratory Director John Grossenbacher's discussions with national leaders, customers, regional groups and you – INL employees – he's been passionately sharing the vision for this new laboratory. That vision is to become the pre-eminent nuclear RD&D

laboratory in 10 years; be a major center for national security technology development and demonstration; be a multiprogram national laboratory; and foster academic, industry, government and international collaborations to produce the investment, programs and expertise to assure the vision. The National and Homeland Security

See **DIVISION**, page 5

FUEL (continued from page 1)

Under the direction of DOE's National Nuclear Security Administration (NNSA), the Global Threat Reduction Initiative will systematically and comprehensively address the myriad proliferation threats facing the world. Specifically, the Initiative will:

- Partner with Russia to repatriate Russian-origin fresh HEU fuel from Russian-supplied research reactors, and work with Russia to accelerate and complete the repatriation of Russian-origin spent fuel from these same reactors.
- Accelerate and complete repatriation of eligible U.S.-original research reactor spent fuel from locations around the world.
- Convert the cores of civilian research reactors that use HEU to low enriched uranium fuel, not just in the United States, but throughout the entire world, and
- Identify other nuclear and radiological materials and related equipment not yet covered by existing threat reduction efforts, and rapidly address facilities to eliminate gaps that would enable a terrorist to acquire materials.

INL is helping to meet the great challenge taken on by Abraham. Its more than 50 years of nuclear science and engineering leadership has placed our scientists at the forefront of GTRI efforts. "60 Minutes" broke a story on Russian fuel repatriation, highlighting INL scientist Igor Bolshinsky's contributions. Mitch Meyer may not have the visibility of the national media – yet – but he and his team are tackling a tough issue, higher-density low enrichment fuel development.

RERTR and INL

The Reduced Enrichment for Research and Test Reactors



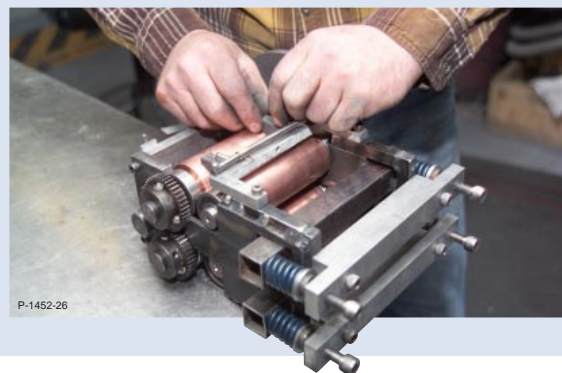
Multiple prototypic fuel elements will be test-irradiated to prove that the fuel performs flawlessly.

Ron Briggs watches as Ben Cowan removes foil from the rolling mill.



Mitch Meyer examines the foil strip held by Ben Cowan. The team has irradiated more than 175 test plates and will be conducting more tests this spring.

In the Electron Microscopy Lab, Dennis Kaiser analyzes weld quality on irradiated fuel samples (below). INL engineer Gaven Knighton designs and builds specialized equipment used to make the low-enriched fuel (bottom).



(RERTR) program has been operating since 1978. It was brought under the GTRI umbrella to more closely coordinate its activities with other nonproliferation programs. The RERTR program develops advanced, high-density LEU fuels to allow conversion of reactors; provides assistance to research reactors for feasibility studies, conversion analyses, and licensing support; converts reactors to the use of LEU; and develops and demonstrates LEU-based medical isotope production techniques. LEU, defined as less than 20 percent enrichment in U-235, is not weapons grade material.

The Office of Defense Nuclear Nonproliferation reports that to date, 39 reactors in 22 countries and the United States have been fully or partially converted from HEU to LEU. They state that 20 new research reactors using LEU fuel have been built or planned in 15 countries. Cumulatively, these efforts account for enough material to manufacture more

than 100 nuclear weapons. But the program still has a long way to go, with 66 research reactors still targeted for conversion before the end of fiscal year 2014.

About 35 of these reactors can be converted using currently qualified fuels, some of which were

developed by the RERTR program. But new fuels must be created for the remaining 31 reactors, and that is where the INL's strength in nuclear technology development comes in.

Meyer's team is working cooperatively with five countries



The INL team brings dedication, scientific expertise and matchless research facilities to help DOE and NNSA meet their goals. (Back row, left to right) Curtis Clark, Pat Hallinan, Gaven Knighton, Dennis Kaiser, and Dan Wachs. (Front row, left to right) Mitch Meyer, Ben Cowan, and Ron Briggs. Not pictured are Karen Moore and Dana Meyer.

to develop new fuels with very high uranium density. The high uranium density offsets the lower enrichment of U-235 in the fuel and provides the same or higher fissile atom density. The RERTR program strategy is to enable conversion with no significant changes in reactor economics, safety or performance.

The fuel development strategy is as detailed and exacting as the science involved in it: defining fuel testing requirements, fabricating fuel, conducting irradiation testing, modeling fuel behavior and providing technical support for core conversion.

The team has irradiated more than 175 test plates in five tests conducted at the Advanced Test Reactor – INL's unparalleled research reactor. Three additional tests, RERTR-6, -7 and -8 miniplate tests are scheduled, -6

beginning this spring. RERTR-6 is a scoping test at moderate heat flux and burn up; -7 will test at higher power and burn up, and -8 will be a short duration, high-power test. After the miniplate tests are completed, full-size plates will be irradiated followed by irradiation of multiple prototypic fuel elements to prove that the fuel performs flawlessly.

Meyer's INL RERTR team is also responsible for supplying fuel for reactor conversions. In the United States, six university reactors can be converted to LEU, and INL will play a key role in these conversions, beginning with the University of Florida and Texas A&M University this year.

Some foreign reactors will also require conversion assistance and INL will be there too, ensuring

that the transition from HEU fuel to LEU fuel goes smoothly for these reactors. The work on foreign reactor conversions is closely coordinated with other GTRI components – the Foreign Research Reactor Spent Fuel Acceptance Program and the Russian Research Reactor Fuel Return Program – of “60 Minutes” fame.

This combined program of fuel development and fuel supply requires close coordination with the program sponsor, national laboratories, other GTRI components and host research reactor countries. It also requires a lot of travel – the 66 reactors that are targeted for conversion are located in 25 countries from Argentina to Kazakhstan.

Conversion of Russian reactors is also important as evidenced by talks between President Bush

and President Putin at the recent Bratislava summit, where both committed to a joint fuel development program.

“Almost everyone agrees that reactor conversion to low enrichment is the right thing to do,” said Meyer. “Many of the countries that we work with consider their reactors to be a national asset. With this program, they will be able to operate their facilities with much less risk, for everyone.”

RERTR is one of the cornerstones of the Global Threat Reduction Initiative. Its goals are lofty. INL is bringing dedication, scientific expertise and matchless research facilities to help DOE/ NNSA meet these goals.

Mitch Meyer
Mitchell.Meyer@inl.gov



Terrorist incidents such as this damaged tower in Iraq could be prevented with INL's transmission line sensor (photos courtesy of Power Engineers, Inc.).

Sensing Trouble

High-voltage towers, looking like a legion of gigantic Lego robots, march across the nation's landscape carrying millions of watts of power on their outspread limbs. American Electric Power alone reports that it owns 39,000 miles of transmission lines crisscrossing 11 states while servicing more than five million customers. Multiply this by the hundreds of utility companies large and small that service industry and homes, and one realizes the miles of transmission lines is staggering.

Many of these miles, particularly in the West, track across remote and unpopulated areas – seldom visited and hard to maintain. And due to diverse factors such as where the power is generated and deregulation, a tower and a line may service customers hundreds of miles away.

Transmission lines are one component of the power grid, much of which was built in the middle of the last century. Extremes of nature can play havoc on this aging infrastructure. High winds and ice can bring down lines and disrupt power. But in the last few years, another threat began looming on the horizon for the power industry – terrorism.

In the past months, several acts of apparent domestic terrorism made headlines. In Wisconsin, someone removed bolts from the base of a high-voltage transmission tower, not only taking it down, but also causing damage to a second tower on which it fell. Seventeen thousand customers lost power. In California, Michael Devlyn Poulin pled guilty to two felony counts of damaging towers near Redding and Kalamath Falls, Ore. Poulin said he wanted to highlight the threat to the nation's electrical power and claimed he removed bolts from eight high-voltage structures in four states: California, Oregon, Washington and Idaho.

This isn't just an American problem, either. Canadian TV reported an apparent bomb attack on a Hydro-Quebec tower that delivers electricity from James Bay to the Boston area.

Industry and Homeland Security recommendations to utilities include increasing awareness, ground patrols and aerial surveillance; peening or tack welding bolts; and coordination with local law enforcement.

INL researchers John Svoboda and Bob Polk are developing a sensor that may soon be added to the arsenal of protective options.

They are testing a sensor platform capable of detecting tower tampering, and relaying this information to the Power Transmission Control Center.

Sensor Platform

Svoboda and Polk based their design on sensor platforms used for remote geosensing at the Nevada Test Site and the Gilt Edge Gold Mine in South Dakota. They recognized that environmental monitoring shared some requirements with utility security. In addition to remoteness, both applications need to run autonomously, be reliable and operate on available power without batteries.

The engineers responded to these requirements with a system that is self-powered and virtually maintenance free. The technology consists of a series of small, inexpensive, low-power electronic sensor platforms mounted on conductors adjacent to each tower/pole of an electric power transmission or distribution line.

In addition to the sensors – accelerometers, infrared detectors or acoustic devices among others – the platform includes a small electronic package consisting of a sensor interface, a micro power processor, an inductively coupled

energy conversion/storage system and a low-power RF transmitter/receiver. The prototype is less than 12 inches long from antenna to base and can be designed to resemble transmission line components such as vibration dampers.

When an event is recorded by the sensor indicating tower tampering, the platform wakes up and sends a message containing event information and tower identification to adjoining towers. The platforms on the adjoining towers wake up in response and transmit to the next towers. The process continues until the message reaches the end of the line, where it can be communicated to a central monitoring location.

The whole system is powered from the magnetic fields that are produced from the wire's alternating current. The power

INL researchers John Svoboda and Bob Polk are developing a sensor that will help surveil high-voltage structures.

P-1408-10



generated is stored for use by the sensors, processor and RF transmitter/receiver. Enough energy is stored to allow several minutes of operation after loss of transmission line power.

Sensor Testing

Svoboda and Polk didn't have to travel far to conduct the initial tests on their design, only about a mile from their sensor lab in Idaho Falls to the banks of the Snake River, where Idaho Falls Power generously supplied technical support and power lines. "We could have tested on INL's power distribution system," said Svoboda, "but the more we work with utilities, the better we understand their requirements and can supply a tool that is practical and cost-effective."

Svoboda and Polk conducted a series of vibration characterization impact tests to confirm the system could identify transmission line tampering and transmit the data. Tests on the low-voltage line were successful. Now, the engineers are working to collaborate with a utility to place sensors on a high-voltage line, the economic target for the sensor platforms. High-voltage towers cost more than low voltage lines, and the loss of a tower would have greater impact to customers and the grid.

While security is the primary driver, the sensors could be capable of detecting other abnormal conditions of concern to utilities such as galloping conductors and fires below the towers.

And regardless of the application, low cost is also an essential requirement for the sensor to have utility and acceptance. Conductor monitors on the market today are relatively complex and expensive, and are not suited for a mass application such as this. The target cost for the unit is about the same as a typical high-voltage insulator string.

As Svoboda and Polk continue to develop the system, they recognize other homeland security applications.

"There is evidence that the sensors could detect movement of vehicles or even low-flying planes," said Polk. "Our design using energized systems as the power source, provides space and power for a number of sensors, including miniature acoustic, chemical, biological or nuclear sensors."

They have more work to do on the design, refining algorithms and testing corona discharge effects – heard as the pops and snaps near high power lines resulting from ionization. They are also working with an infrared lens supplier to develop a transmission line application-specific IR lens. But it won't be too long until the next time a vandal or terrorist tries to unbolt a tower, an INL sensor sends out the alert.

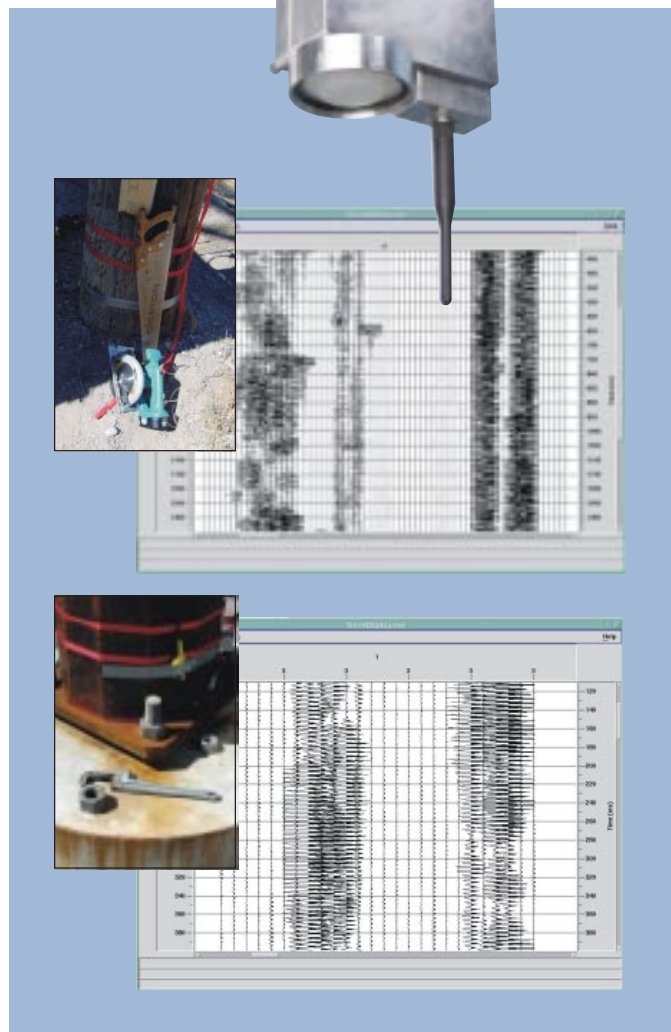
Bob Polk

Robert.Polk@inl.gov

John Svoboda

John.Svoboda@inl.gov

INL's sensor is a compact transmitting device that hangs from the power line (right). Various forms of tampering produce unique signatures that can be identified, such as sawing or unbolting (below).



DIVISION *(continued from page 1)*

Division will play a vital role in achieving this vision.

During the past weeks, I've been meeting with our customers across the country to better understand their requirements. I've visited with corporate, law enforcement and government leaders in

Boise to help open a dialogue on ways INL can better meet host-state expectations. I've also been working with INL managers and staff to learn more about our programs and capabilities. Now, we're developing the strategy that will help us acquire a world-class reputation in supporting our National and Homeland

Security customers achieve mission-critical outcomes. I've shared with you the key elements of our strategy – develop synergism with INL's core mission through nonproliferation and safeguards; capitalize on our unique site and physical assets; build on recognized areas; leverage growth through collaboration and partnerships,

attract nationally recognized staff and most important, perform exceptionally well on current programs.

You are essential to our success and I ask for your continued commitment to help us establish a world-class reputation.

Idaho National Laboratory is poised for greatness. Let's work together to achieve it!



INL's Julio Rodriguez explains the components of a vendor's system to Eric Byres, a British Columbia Institute of Technology control system researcher.

West. These interconnected pipe and transmission lines provide a constant flow of energy products from Canada to the United States and visa versa.

In 2002, Canada exported nearly \$50 billion of energy products to the United States. An estimated four percent of that, or \$1.8 billion, was in the form of electricity. Canada provides electrical power to portions of New England, New York, the Pacific Northwest and California.

The interconnectivity of the critical infrastructures that the United States and Canada share is good for consumers, but it has had the unintended effect of creating a target for terrorists. The vulnerabilities of these systems are not just physical, but also cross into the virtual realm.

Cyber security experts have long made the case that the digital automation systems that control, operate and monitor the massive infrastructure systems – like the electrical power grid and the thousands of miles of shared natural gas pipelines – lack modern and sufficient cyber security measures. Electric power, unlike other energy sources, must be created in real time and can't be stored. If a natural disaster, terrorist attack or equipment

International Relations

INL Critical Infrastructure Department expands to global audience

Contributed by Ethan Huffman

According to the U.S. Department of Homeland Security, the United States shares more than 5,000 miles of border with Canada. It is the largest and most open border in the world, with more than 1,000 joint air, land and sea entry ports. Attempts to secure this border, and prevent the inflow of terrorists into the United States, has been a constant and scrutinized problem for the federal government.

Since 9/11, billions of dollars have been directed toward increasing the level of physical security along the U.S.-Canadian border.

According to the State Department, in 2003 an additional 375 border patrol agents were added to the northern border, bringing the total number of agents to more than 1,000. Additionally, new restrictive devices and protocols such as concrete barriers, armed-guard stations and identification measures have also been put into place to prevent terrorists from

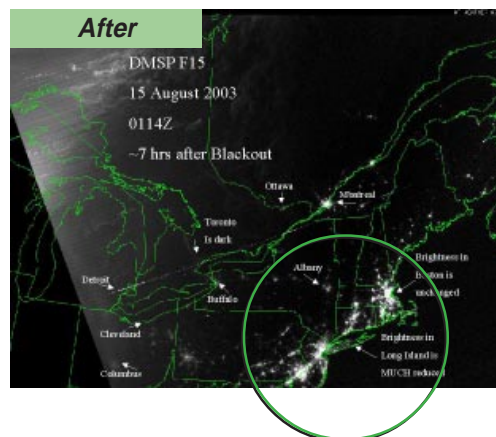
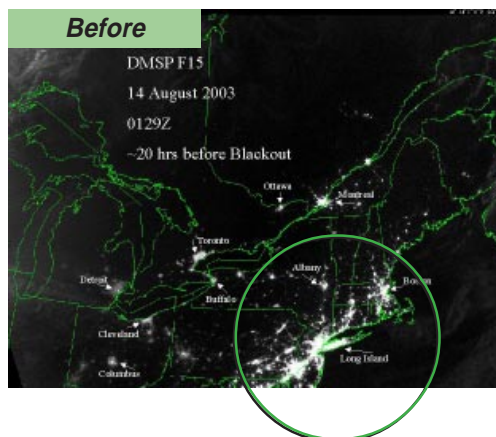
entering either nation.

Yet with all the focus on securing the physical border, few people realize that in terms of critical infrastructures, such as the electrical power grid and natural gas pipelines, a border doesn't exist. That fact became clearly evident during the August 2003 blackout, which originally began in Ohio, but

within minutes left upwards of 10 million U.S. and Canadian residents without power.

According to the Canadian Embassy, the United States and Canada are interconnected by 35 cross-border natural gas pipelines and 51 cross-border electric transmission lines, as well as several shared hydropower facilities on the border in the

The August 2003 blackout originally began in Ohio, but within minutes left upwards of 10 million U.S. and Canadian residents without power.



failure occurs in Canada, millions of Americans could be left without essential services like power, emergency services and running water.

INL works with BCIT

INL and the British Columbia Institute of Technology (BCIT) are looking at cutting-edge ways to protect both nations' critical infrastructures, including the power grid, from a cyber intrusion.

Last November, four INL employees met with members of BCIT's industrial cyber security team in Canada to discuss future collaborations between the two organizations. The trip was funded as part of the DHS commitment to control systems security to U.S. critical infrastructures.

According to Alan Snyder, who coordinates control system testing for INL's SCADA Test Bed, cyber space is similar to the U.S./Canada border. "There are no boundaries to cyber security. If a cyber attack penetrates a Canadian control system, it has a good chance of causing problems in the United States."

Snyder and SCADA and Cyber Security experts at INL are working with BCIT to outline long-term objectives for critical infrastructure protection between both countries.

"The hope is that in the long term, we'll create a dialogue of two-way communication between both countries," said Snyder.

"Then, we can share data, develop tools, and foster an environment where cyber vulnerabilities are quickly identified and mitigated."

Those statements are also supported by Eric Byres, a BCIT Control System researcher.

"International participation in this area is absolutely essential," said Byres. "The large companies that we work with have locations all over the world, and their resources provide energy

products to people everywhere, so the threat is not localized."

Byres hopes that BCIT's collaboration with INL will eventually yield open communication and data sharing.

"I think this relationship will be particularly beneficial in terms of attack trees, network modeling and immulation," said Byres.

"BCIT and INL have a tremendous resource of information and technology. I hope we can take advantage of both skill sets and come up with some inventive ways for solving this problem."

This is something that Byres has seen work successfully in other countries and even within the highly competitive industrial sectors.


"If you look at companies like British Petroleum and Chevron/Texaco, they both have created awareness campaigns between the IT and control system sectors, and cross training programs that they share with other companies," said Byres.

One of the ways that INL hopes to involve Byres and BCIT is by including them in the testing of some control systems and component products. According to Snyder, several control system manufacturers are based in Canada, and having someone familiar with Canadian protocols and regulations participate in the evaluations would be a beneficial step to ensure proper security measures are in place in both nations.

In March, INL cyber security and control system experts attended a symposium and workshop at BCIT with several national and international utility sector representatives.

Julio Rodriguez
Julio.Rodriguez@inl.gov

Rob Hoffman
Robert.Hoffman2@inl.gov



Japan looks to INL to increase control systems security

The potential for a cyber intrusion on our nation's critical infrastructures poses a significant threat to national security. But the concept of cyber warfare is universal. In fact, many of the control systems that are tested and analyzed as part of INL's Critical Infrastructure Protection initiative operate power grids, transportation systems and telecommunications networks both at home and abroad.

This reality has led INL to formulate working relationships with international control system vendors, manufacturers and research collaborators who all agree that improving cyber security for control systems is a global necessity.

In February, Critical Infrastructure Assurance Department Manager Julio Rodriguez and Cyber Security Research Department Manager Rob Hoffman spent five days in Tokyo, Japan, at the Central Research Institute of Electric Power Industry (CRIEPI).

Similar to the U.S. Electrical Power Research Institute, CRIEPI is an international energy research organization — but with close ties to the Japanese government — that works to provide analysis and emerging solutions to the private sector. CRIEPI's interest in INL's capabilities is largely due to the work being conducted in cyber security.

"CRIEPI is a large-scale research institution that performs tests on transformers

and switches," said Hoffman. "What makes our capabilities significant, and what interests CRIEPI, is that we've added a cyber security element to our testing of control systems."

At last year's KEMA conference in Idaho Falls, three CRIEPI research engineers met with Rodriguez and Hoffman to get a first-hand look at INL's newly established control system testing facilities set up jointly by the Department of Energy and the Department of Homeland Security. As recent as January, CRIEPI engineers again visited INL to see the progress made at the facilities and to invite management to visit CRIEPI facilities in Japan.

Dartmouth College's Institute for Security Technology Studies funded the trip for two purposes. First, CRIEPI is hoping INL will perform tests and develop solutions for a major Japanese control system vendor. And second, CRIEPI has expressed interest in setting up a testing facility in Japan that would be modeled after the facility at INL.

"Our relationship with CRIEPI is especially important in this area because critical infrastructure protection is an international problem," said Rodriguez. "In fact, much of the infrastructure in place in the United States relies on foreign vendors and equipment, so having a good relationship with international parties benefits us, too."

In March, INL sent CRIEPI a proposal to initiate the delivery of vendor equipment to the lab's control system security facilities. INL engineers plan to begin testing and analysis on a Japanese system later this year.



Counterintelligence CORNER

Espionage Investigations

Contributed by C. Gene Johannes
Counterintelligence Officer

Why was Aldrich Ames able to spy for the Soviet Union against the United States from 1985 to 1994? How was Robert Hanssen able to spy on the United States from 1979 to 2001 without being caught?

These questions help bring to light some of the basic differences between an espionage investigation and a criminal investigation. A criminal investigation usually begins with a crime scene, which contains evidence that a crime has been committed. An espionage investigation usually begins with a “possible” indicator that an act of espionage may or may not have taken place.

Examples of indicators include the following: John Doe paid cash for a home, far in excess of his known salary. Or, while on foreign travel, a scientist sees a prototype that looked much like a U.S. prototype and we believe

our research is 10 years ahead of them. Or, Jane Smith has taken more foreign trips than she indicated on her security form.

While these circumstances create suspicions, when explored, they

may have perfectly legitimate explanations. Or, they could be indications that an act of espionage has taken or is taking place. Hence, intelligence investigators are generally investigating the indication or possibility of a crime, rather than an actual known crime.

The case of Aldrich Ames was an oddity in that the intelligence community knew there was a problem when the majority of covert intelligence sources in the Soviet Union were imprisoned or executed in a short period of time. Even with this knowledge, it took approximately two years of internal investigations to narrow the search down to the agency where the leaked information originated.

Investigators then determined who had access or knowledge to these intelligence sources. It took another two years of sifting through and eliminating individuals with access until a

short list of “possible” suspects was developed. The investigators focused on the “possible” suspects until the actual spy was identified.

In the Ames case, as in many investigations, there were indicators that something just didn’t look right. Among other indicators, there was unexplained affluence.

A study was conducted of convicted espionage agents that revealed the presence of one or more of the following indicators: revenge, unexplained affluence, seeking information without a need to know, working odd hours, excessive debt, alcohol or drug abuse, emotional instability, skeleton in the closet, and unexplained travel.

The importance of reporting possible indicators or those things that just don’t look right cannot be overemphasized. Most of reported indicators have legitimate explanations and are resolved with a discrete and unobtrusive inquiry. A few reported concerns turn into an inquiry, and an even smaller number of concerns lead to a full investigation. However, it is these reported indicators that often help catch spies.

Without a crime scene, the reporting of employee concerns is vital to countering the collection of information by foreign individuals, companies, countries and terrorists.

Remember JDLR – If it “Just Doesn’t Look Right,” report it. Idaho National Laboratory employees can contact the Counterintelligence Office at: (208) 526-2223/4023/3661.

Unlike a criminal investigation, an espionage investigation is usually based on a possible indicator rather than an actual crime scene.



NEED TO KNOW is a publication of the National and Homeland Security Division of Idaho National Laboratory. INL is a U.S. Department of Energy national laboratory and performs work in each of DOE's strategic mission areas – environment, energy, science and defense. Battelle Energy Alliance manages and operates the laboratory for DOE. Requests for additional copies, story ideas or questions should be directed to the editor at (208) 526-1058, Kathleen.Gatens@inl.gov.

Editor Kathy Gatens
Graphic artist David Combs
Photographer Chris Morgan
Copy editing Rick Bolton
Research Steve Paschke
Visit our website at:
www.inl.gov/nationalsecurity

